IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	1:18-cr-410 (LMB)
SEITU SULAYMAN KOKAYI,	)	
	)	
Defendant.	)	
	)	

MEMORANDUM OPINION

Defendant Seitu Sulayman Kokayi ("Kokayi") was charged with two counts of coercion and enticement of a juvenile to engage in unlawful sexual activity in violation of 18 U.S.C. § 2422(b) and one count of transfer of obscene materials to a minor in violation of 18 U.S.C. § 1470 [Dkt. No. 29] after the Federal Bureau of Investigation ("FBI") became aware that he was having sexual conversations with a female minor via text messaging and FaceTime.

On November 9, 2018, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), the government provided notice to Kokayi and the Court that it "intends to offer into evidence, or otherwise use or disclose in any proceedings in [this case], information obtained or derived from electronic surveillance and physical searches conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 ('FISA'), as amended, 50 U.S.C. §§ 1801-1812 and 1821-1829." Dkt. No. 33. The underlying FISA applications and orders are classified. On December 17, 2018, without having been able to see the relevant FISA applications, defendant filed a Motion to Suppress Electronic Surveillance Obtained Without a Warrant and Without a Finding of Probable Cause of Criminal Conduct, and for Disclosure of the FISA Applications to Defense [Dkt. No. 43] ("Def. Mem."). Defendant argues that the underlying FISA applications and other materials should be disclosed to defense counsel so that counsel can provide effective assistance, emphasizing that the relevant

statutory provisions permit such disclosure under certain circumstances. In addition, defendant claims that the government's FISA evidence should be suppressed because the defendant was not an "agent of a foreign power," the FISA applications were likely predicated on protected First Amendment activities, normal investigative techniques could have been employed, and the required minimization procedures may not have been followed.

The government has filed a classified opposition brief and the relevant FISA materials have been submitted under seal for in camera, ex parte review [Dkt. No. 66] ("Gov. Opp'n"). The government concurrently filed an affidavit signed by the Attorney General claiming that disclosure of the FISA materials or an adversary hearing concerning them would harm the national security of the United States. Dkt. No. 66-1. The affidavit also explains that pursuant to 50 U.S.C. §§ 1806(f) and 1825(g) the Court must conduct an in camera, ex parte review of the documents relevant to defendant's motion. Substantively, the government argues that "the electronic surveillance and physical search at issue in this case were both lawfully authorized and lawfully conducted in compliance with FISA" and that disclosure to the defendant is not authorized "because the Court can make an accurate determination regarding legality without disclosing the FISA materials or portions thereof." Gov. Opp'n 3.

I. OVERVIEW OF FISA

FISA was enacted in 1978 to establish a framework under which the executive branch "could conduct electronic surveillance for foreign intelligence purposes without violating the rights of citizens." United States v. Hammoud, 381 F.3d 316, 332 (4th Cir. 2004) (en banc), vacated on other grounds, 543 U.S. 1097 (2005).[1] Under FISA, the Chief Justice of the United

[1] Although FISA initially pertained only to electronic surveillance, see 50 U.S.C. §§ 1801–1812, it has since been expanded to include physical searches, see id. §§ 1821–1829.

States designates eleven federal district court judges to sit as members of the Foreign Intelligence Surveillance Court ("FISC"). See 50 U.S.C. § 1803(a)(1). Subject to certain exceptions,[2] the executive branch must receive advance approval from a FISC judge for all electronic surveillance of a foreign power or its agents. Hammoud, 381 F.3d at 332. To secure such approval, the government must file an ex parte, under seal application with the FISC. 50 U.S.C. § 1804. For electronic surveillance,[3] this application must be approved by the Attorney General and include, among other things, the identity or a description of the target of the surveillance and a statement of the facts and circumstances supporting probable cause to believe that "(A) the target of the electronic surveillance is a foreign power[4] or an agent of a foreign power;[5] and (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power," as well as a detailed description of the information sought and the types of communication or activities subject to

---

[2] The Attorney General may issue an emergency order authorizing FISA surveillance under certain circumstances, see 50 U.S.C. § 1805(e)(1); however, the government must submit an application to a FISC judge "as soon as practicable, but not later than 7 days after the Attorney General authorizes such surveillance," id.

[3] The requirements for physical surveillance are similar but include additional requirements that the application detail the facts and circumstances justifying an applicant's belief that "the premises or property to be searched contains foreign intelligence information" and that each "premise or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from" the target. 50 U.S.C. § 1823(a)(1)–(8), (a)(3)(B), (C).

[4] A "foreign power" is defined as a "foreign government or component," entity controlled by a foreign government, "group engaged in international terrorism or activities in preparation therefor," "foreign-based political organization," or entity that is "engaged in the international proliferation of weapons of mass destruction." 50 U.S.C. §§ 1801(a)(1)–(7), 1821(1).

[5] A non-U.S. person is an "agent of a foreign power" if her or she "acts in the United States as an officer or employee of a foreign power"; "acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States"; or "engages in international terrorism," "international proliferation of weapons of mass destruction," or activities in preparation therefor. 50 U.S.C. § 1801(b)(1). The definition of "agent of a foreign power" is similar for a U.S. person, but the relevant behavior must be done "knowingly." See id. § 1801(b)(2).

surveillance. See id. § 1804(a)(2)–(3), (5). In addition, the application must contain a certification from a high-ranking executive branch official stating that "the certifying official deems the information sought to be foreign intelligence information," "that a significant purpose of the surveillance is to obtain foreign intelligence information," and "that such information cannot reasonably be obtained by normal investigative techniques." Id. §§ 1804(a)(6), 1823(a)(6).[6]

A FISC judge may issue an order authorizing FISA surveillance only upon concluding "that there is probable cause to believe that the target of the surveillance is a foreign power or agent of a foreign power, that proposed minimization procedures are sufficient under the terms of the statute, that the certifications required by § 1804 have been made, and that the certifications are not clearly erroneous." United States v. Squillacote, 221 F.3d 542, 553 (4th Cir. 2000). The order authorizing FISA surveillance must "describe the target, the information sought, and the means of acquiring such information" and also "set forth the period of time during which the electronic surveillance or physical searches are approved, which is generally ninety days or until the objective of the electronic surveillance or physical search has been achieved." United States v. Rosen, 447 F. Supp. 2d 538, 544 (E.D. Va. 2006).

"[O]nce the electronic surveillance or the physical search has been approved, the government must apply the specific minimization procedures contained in the application to the FISC." Id. at 550. Although the specific minimization procedures contained in each application

[6] As defined by the statute, "foreign intelligence information" is that which "relates to . . . the ability of the United States to protect against . . . attack or other grave hostile acts of a foreign power [or agent thereof]. . . sabotage, international terrorism, or . . . clandestine intelligence activities by . . . a foreign power [or agent thereof]." 50 U.S.C. §§ 1801(e)(1), 1821(1). It also includes "information with respect to a foreign power or territory that relates to . . . the national defense[,] security . . . [, or] foreign affairs of the United States." Id. § 1801(e)(2).

are classified, the statute requires that such minimization procedures be "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. §§ 1801(h), 1821(4)(A). As explained by the Foreign Intelligence Surveillance Court of Review:

> By minimizing acquisition, Congress envisioned that, for example, where a switchboard line is tapped but only one person in the organization is the target, the interception should probably be discontinued where the target is not a party to the communication. By minimizing retention, Congress intended that information acquired, which is not necessary for obtaining, producing, or disseminating foreign intelligence information, be destroyed where feasible. Furthermore, even with respect to information needed for an approved purpose, dissemination should be restricted to those officials with a need for such information.

In re Sealed Case, 310 F.3d 717, 731 (Foreign Int. Surv. Ct. Rev. 2002) (emphasis in original) (internal quotation marks omitted). But 50 U.S.C. § 1801(h)(3) expressly states that the government is not required to minimize information that is "evidence of a crime."

"Although FISA is chiefly directed to obtaining 'foreign intelligence information,' the Act specifically contemplates cooperation between federal authorities collecting [FISA material] and federal law enforcement officers" and "explicitly allows the use of evidence derived from FISA surveillance and searches in criminal prosecutions." Rosen, 447 F. Supp. 2d at 544. If the government intends to use FISA evidence in the criminal trial of an "aggrieved person," it must notify the aggrieved person and the court of this intent. 50 U.S.C. §§ 1806(c), 1825(d). An aggrieved person "may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that the information was unlawfully acquired; or the surveillance was not made in conformity with an order of authorization or approval." Id. §§ 1806(e), 1825(f). Upon such a motion, "if the Attorney General files an affidavit under oath that disclosure or an

adversary hearing would harm the national security of the United States," the district court "shall" review the relevant FISA materials in camera and ex parte "to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." Id. §§ 1806(f), 1825(g). The court may disclose the FISA materials or portions thereof to the aggrieved person "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." Id. § 1806(f); see also id. § 1825(g).

In the Fourth Circuit, the district court's review of FISA materials is de novo, Squillacote, 221 F.3d at 554, and, given that "review is ex parte and thus unaided by the adversarial process," the review should be both "searching and conducted with special care," Rosen, 447 F. Supp. 2d at 545. But, just as the FISC applies a "clearly erroneous" standard to the specification, 50 U.S.C. §§ 1805(a)(4), 1824(a)(4), the district court applies a "strong presumption of veracity and regularity" to the FISA application, United States v. Hassan, 742 F.3d 104, 139 (4th Cir. 2014). As with probable cause to believe that criminal activity is occurring, probable cause to believe that the target of FISA surveillance is an agent of a foreign power "is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." Hammoud, 381 F.3d at 332 (quoting Illinois v. Gates, 462 U.S. 213, 232 (1983)). In evaluating probable cause, a judge must "'make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . , there is a fair probability' that the search will be fruitful." Id. (alteration in original) (quoting Gates, 462 U.S. at 238). Stated differently, "[p]robable cause means more than bare suspicion but less than absolute certainty that a search will be fruitful." Id. (quoting Mason v. Godinez, 47 F.3d 852, 855 (7th Cir. 1995)).

II. DISCUSSION

As a threshold procedural matter, defense counsel contends that he needs access to the FISA material to develop suppression arguments. Def. Mem. 1. This argument is unpersuasive. FISA expressly states that a court "shall" review FISA materials ex parte and in camera "if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States." 50 U.S.C. §§ 1806(f), 1825(g). The Attorney General has submitted such an affidavit [Dkt. No. 66-1], and it is not for the Court to second-guess the determination of a top executive branch official with access to a broad range of intelligence that disclosure of the FISA materials would be harmful to national security. Cf. C.I.A. v. Sims, 471 U.S. 159, 180 (1985) ("[I]t is the responsibility of the Director of Central Intelligence, not that of the judiciary, to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the Agency's intelligence-gathering process."). FISA's ex parte and in camera review procedures are not, as defendant claims, "antithetical to the adversary system that is the hallmark of American criminal justice." Def. Mem. 17. To the contrary, they are congressionally authorized, and their constitutionality has been affirmed by the Fourth Circuit, United States v. Pelton, 835 F.2d 1067, 1075–76 (4th Cir. 1987) ("We find the provisions of FISA to be 'reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens,' and therefore compatible with the Fourth Amendment." (citing United States v. U.S. Dist. Court for E. Dist. of Mich.., 407 U.S. 297, 323 (1972))), as well as every federal court that has considered the matter, Gov. Opp'n 17–18 (collecting cases).

The exception to the requirement of ex parte, in camera review applies "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. §§ 1806(f), 1825(g).

> [S]uch disclosure is "necessary" only where the court's initial review of the application, order, and fruits of the surveillance indicates that the question of legality may be complicated by factors such as "indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order."

United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982) (quoting S. Rep. No. 95–701, at 64 (1978)). Reviewing ex parte applications to determine whether they establish probable cause is a traditional function of courts and, unsurprisingly, only one court has ever concluded that defense input was necessary to determine the legality of FISA materials: that decision was overturned. Gov. Opp'n 18–19.[7] This case is no exception and falls in line with every other court to consider the matter. Having reviewed the FISA applications, orders, and warrants, the Court finds that they contain no facial inconsistencies, ambiguities, or inaccuracies and that disclosure is not necessary to make an accurate determination of the legality of the surveillance.

On the merits, defendant attacks the legality of the FISA applications, arguing that the Court should suppress all the FISA evidence because it was collected in violation of FISA and the Fourth Amendment. Def. Mem. 3. This necessarily speculative contention is based on defendant's claims that the applications failed to establish a "reasonable, particularized ground for belief that the defendant qualified as an agent of a foreign power." id. at 7, or that the underlying information used to satisfy the FISA probable cause standard is inaccurate or

[7] The district court in United States v. Daoud, No. 12-CR-723, 2014 WL 321384 (N.D. Ill. Jan. 29, 2014) found that disclosure "may be necessary" and ordered the disclosure of FISA materials to defense counsel despite being capable of making the determination itself. Id. at *3. The Seventh Circuit subsequently overturned that decision to disclose. United States v. Daoud, 755 F.3d 479, 485 (7th Cir. 2014) ("Because [the district court judge] was 'capable' of making the determination, disclosure was not 'necessary' under any definition of that word.").

unreliable[8] or contains intentional or reckless falsehoods or omissions,[9] id. at 8–13.

All these arguments amount to an attack on probable cause. Based on its review of the materials, the Court finds that there was probable cause to believe that certain identified organization(s) were a "foreign power" within the meaning of 50 U.S.C. § 1801(a), which includes a "group engaged in international terrorism or activities in preparation therefor," and that the target(s) knowingly acted for or on behalf of those organizations, or knowingly aided or abetted those organizations and were therefore "agent(s) of a foreign power" under 50 U.S.C. §§ 1801(b)(2), 1821(1). In addition, the applications established probable cause to believe that each facility or place at which electronic surveillance was directed "[was] being used, or [was] about to be used, by a foreign power or an agent of a foreign power" and that the premises to be physically searched were, or were about to be, owned, used, or possessed by, or were in transit to or from, the target(s).

Defendant's next argument is that the FISA applications may have been improperly predicated on protected First Amendment activities. Def. Mem. 8, 10. This argument is supported by neither facts nor law. FISA provides that "no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States." 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A). The critical word in that provision is "solely." As the Rosen

[8] Defendant argues that the underlying information in the FISA application may have been intercepted pursuant to the Terrorist Surveillance Program, a warrantless wiretapping program instituted in 2001, or the FISA Amendments Act of 2008. Def. Mem. 9–10.

[9] Under Franks v. Delaware, 438 U.S. 154 (1978), the target of a search may obtain an evidentiary hearing concerning the veracity of information set forth in a search warrant affidavit if the target "makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included" and if the allegedly false statements were "necessary to the finding of probable cause." Id. at 156–57.

opinion made clear, as a statutory matter, "[f]rom this plain language, it follows that the probable cause determination may rely in part on activities protected by the First Amendment, provided the determination also relies on activities not protected by the First Amendment." 447 F. Supp. 2d at 548.[10] From a constitutional perspective, just as it is entirely consistent with the First Amendment to make "evidentiary use of speech to establish the elements of a crime or to prove motive or intent" during a criminal proceeding, Wisconsin v. Mitchell, 508 U.S. 476, 489 (1993); see also United States v. Hassan, 742 F.3d 104, 127–28 (4th Cir. 2014) ("[T]he First Amendment was no bar to the government's use of the appellants' speech to demonstrate their participation in the charged conspiracies."), so too is it appropriate to use speech to establish probable cause to believe that a target of FISA surveillance is an agent of a foreign power. Therefore, even if defendant were a/the target, it would have been permissible for the FISA application to refer to First Amendment-protected activities, provided that there was other evidence of prohibited activity.

Defendant also argues that the purpose of the FISA surveillance may have been "criminal in nature," rather than to collect foreign intelligence information. Def. Mem. 13. "Although FISA is chiefly directed to obtaining 'foreign intelligence information,' the Act specifically contemplates cooperation between federal authorities collecting [FISA material] and federal law enforcement officers" and "explicitly allows the use of evidence derived from FISA surveillance and searches in criminal prosecutions." Rosen, 447 F. Supp. 2d at 544. After having reviewed the FISA materials, it is clear to the Court that the purpose of the FISA surveillance was to collect

[10] FISA's legislative history explains that the statute is "not intended to authorize electronic surveillance when a United States person's activities, even though secret and conducted for a foreign power, consist entirely of lawful acts such as lobbying or the use of confidential contacts to influence public officials, directly or indirectly, through the dissemination of information." S. Rep. No. 95–701, at 29.

foreign intelligence information. It was in the course of that surveillance that evidence of the criminal activity at issue in this case was discovered. Therefore, the applications were proper and the evidence obtained of criminal activity may be used in the criminal trial.

Defendant next argues that the FISA applications may not have included the certifications required under 50 U.S.C. § 1804(a)(6). Def. Mem. 13–14. Under § 1804(a)(6)(E), there must be a statement of the basis for the certifications (i) that the information sought is "the type of foreign intelligence information designated" and (ii) that the information sought "cannot reasonably be obtained by normal investigative techniques." 50 U.S.C. § 1804(a)(6)(E). Because defendant is a United States person, this certification must be measured by the "clearly erroneous" standard. Def. Mem. 14 (citing 50 U.S.C. § 1805(a)(4)). The Court has scrutinized this certification and finds that the information sought is the type of foreign intelligence information designated and could not reasonably have been obtained by normal investigative techniques; therefore, the certification was not clearly erroneous on the basis of the facts submitted.

Defendant requests that the Court "carefully examine the dates, in sequence, of all FISA orders in this case to determine whether there were any lapses of time during which wiretapping continued." Def. Mem. 14. When a FISA order expires, "extensions of an order . . . may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order." 50 U.S.C. § 1805(c)(2). The Court has examined the dates of all FISA orders and warrants and finds that surveillance was authorized at all times.

Finally, defendant argues that "[i]t is possible that the FISA application did not contain adequate minimization procedures, or, if it did, that those procedures were not followed." Def.

Mem. 15. Other than citing the legal basis for the minimization requirement and explaining why minimization is important, defendant provides no basis for this argument. Instead he simply argues that because "the government has provided an incredibly large amount of products of surveillance," disclosure of the "FISA applications, orders, and related materials" is necessary. Id. This argument also fails. As the legislative history makes clear, "Absent a charge that the minimization procedures have been disregarded completely, the test of compliance is whether a good faith effort to minimize was attempted." Rosen, 447 F. Supp. 2d at 551 (citing S. Rep. No. 95–701, at 39). This is because, "[i]n enacting FISA, Congress recognized that 'no electronic surveillance can be so conducted that innocent conversations can be totally eliminated.'" Hammoud, 381 F.3d at 334 (quoting S. Rep. No. 95–701, at 39). In addition, as courts recognize, "it is not always immediately clear into which category a particular conversation falls. A conversation that seems innocuous on one day may later turn out to be of great significance, particularly if the individuals involved are talking in code." Id. Here, the Court finds that the FISA applications incorporated the appropriate minimization procedures, the orders and search warrants issued by the FISC directed the government to comply with those procedures, and the FISA-authorized surveillance and physical search abided by those procedures when applicable and otherwise demonstrated a "good faith effort to minimize the acquisition and retention of irrelevant information." Id.

Lastly, the Court had a question about one aspect of the FISA materials and conducted an ex parte hearing on the record. The government's representations made during the hearing fully satisfy the Court that proper sealing procedures were used.

In sum, the Court finds that based on its de novo, in camera review of the FISA materials and FISC orders and search warrants that the electronic surveillance and physical searches at

issue in this case were lawfully authorized, conducted in compliance with FISA, and did not violate any of defendant's rights.

III. CONCLUSION

For these reasons, defendant's Motion to Suppress Electronic Surveillance Obtained Without a Warrant and Without a Finding of Probable Cause of Criminal Conduct, and for Disclosure of the FISA Applications to Defense [Dkt. No. 43] will be denied by an appropriate Order to be issued with this Memorandum Opinion.

The Clerk is directed to forward a copy of this Memorandum Opinion to counsel of record and CISO Maura Peterson.

Entered this 13th day of March, 2019.

Alexandria, Virginia

/s/
Leonie M. Brinkema
United States District Judge